REMARKS

Please reconsider the application the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-13 and 15-20 are currently pending. Claims 1 and 15 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 15.

Rejection(s) under 35 U.S.C. § 103

MPEP § 2143 states that "[t]he key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious." The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 82 USPQ2d 1385, 1395-97 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. *See* MPEP § 2143. In the Action, the Examiner, in articulating the analysis used to reject the claims under 35 U.S.C. §103, has described the various claimed elements taught and not taught by U.S. Patent No. 6,286,103 ("Maillard"). *See* Action, page 3. Further, the Examiner has described the various claimed elements taught by U.S. Publication No. 2004/0264700 ("Kirkland"), which are not taught by Maillard. *Id.* The Examiner then concludes by asserting that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Maillard and Kirkland. *Id.*

Using the above rationale, the Examiner "must articulate the following: (1) a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference." *See* MPEP § 2143(A). Applicants respectfully submit that the Examiner has failed to do so.

If the Examiner does not produce a *prima facie* case, Applicants are under no obligation to submit evidence of non-obviousness. The initial evaluation of *prima facie* obviousness thus relieves both the Examiner and Applicants from evaluating evidence beyond the prior art and the evidence in the specification as filed until the art has been shown to suggest the claimed invention. *See* MPEP § 2142.

Claims 1-7, 11-13, 15-16, and 19-20

Claims 1-7, 11-13, 15-16, and 19-20 are rejected under 35 U.S.C. § 103(a) as being anticipated by U.S. Patent No. 6,286,103 ("Maillard") in view of US Publ. No. 2004/0264700 ("Kirkland"). This rejection is respectfully traversed as follows.

The claimed invention is directed to communication of a *broadcast message* between a sender/sending system and several receiving systems. Specifically, the claimed invention operates as follows. A sender key Ke is generated on the transmitting side that is never sent to the receiving systems. Each receiving/decoding pair of devices has a first key d1 and a second key d2. In a particular embodiment, the key d1 is the decoder key and the key d2 is the security module key. The decoder key is hardwired and cannot be changed. When a new key Ke is produced at the sender side, for each receiver a new key d2 is calculated and sent through usual means. Thus, for example, Receiver A : determines d1a and calculates d2a = f(Ke, d1a), Receiver B : determine d1b and calculate d2b = f(Ke, d1b), so on and so forth. Finally, each receiver is able to decrypt the broadcast message by the unique combination of d1 and d2, this combination forming a pairing between these two receiving/decoding devices.

Accordingly, the claimed invention requires, in part, a broadcasting system where (i) each receiving decoding system of a plurality of such receiving decoding systems is

configured to descramble scrambled audiovisual data received via the broadcasting network. Thus, the claimed invention requires a one-to-many system in which one transmitted message is *broadcast* to multiple receiving systems. Applicant asserts that neither Maillard nor Kirkland discloses such a broadcast system.

Specifically with respect to Maillard, the Examiner cites column 8, lines 55 to 63 of Maillard as disclosing a receiving/decoding system in a broadcast network that is configured to descramble scrambled data using the key exchange as required by the claimed invention. However, the cited portion of Maillard describes the dialogue between the module and the receiver, the communication of which is entirely different than one required in a broadcast scheme such as that of the claimed invention. The encrypted data stream disclosed in Maillard (*see, e.g.*, Figure 4) is not broadcast, *i.e.*, is not intended to be sent to a plurality of receivers. It is only sent to the *corresponding receiver*. Further, the key Kf of Maillard is present on both sides (3031 and 3033). That is, the key that encrypts the data is the same as the key for decrypting the data. Accordingly, the solution proposed by Maillard is not applicable in the encryption of broadcasted messages, which requires all receivers to have independent means to decrypt the scrambled data. It is therefore not possible to select a key at the sender side to match with a specific receiver.

Kirkland fails to supply that which Maillard lacks, because Kirkland is also directed to a sender and a corresponding receiver, and not to a plurality of receiving systems, of which two devices form a receiving/decoding pair among several such pairs. In fact, such a broadcast mode as described above is not applicable in Maillard and in Kirkland, in which the communication is point-to-point and the keys are chosen according to *a single receiver* configured to receive a message directed to that receiver. Accordingly, the key selected in either

of Maillard and Kirkland does not apply to a broadcast scheme, such as the broadcast system around which the claimed invention is centered. Accordingly, both Maillard and Kirkland fail to supply (i) as required above.

Further, the claimed invention also requires, in part, (ii) a first unique key dedicated to a single device; and (iii) wherein a combination of the first key and a second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data, the encrypted control data being identical for each receiving decoding system. Thus, the claimed invention requires a broadcast system in which a second key is assigned to a portable security module such that the first and second key together make the equivalent of a pairing system key which allows for decryption of common control data. Said another way, the combination of the first and second key, each respectively assigned to a decoder/portable security module pair, allows this one particular pair of devices among several such pairs of devices in the broadcast system to decrypt the control data.

At the outset, Applicant wishes to make of record that the Examiner failed to respond to any of the previous arguments made in the response filed February 14, 2011, with respect to Maillard. While new grounds of rejection were issued in the current Action, the Examiner continues to rely on Maillard for much of the same subject matter for which Maillard was relied upon in the previous Action. Yet none of the Applicant's arguments with respect to Maillard were properly addressed or rebutted by the Examiner. Accordingly, Applicant continues to assert that Maillard fails to disclose or render obvious 1) a single pairing system key that is common to each decoder and portable security module pair, and 2) the combination of the first key and the second key being congruent to the pairing system key.

Specifically, as previously asserted, in Maillard, the EMM containing the exploitation key Cex depends on the personalisation key that corresponds to the unique decoder identity value N. Thus, a different EMM is sent to each portable security module 3020. There is *no* single pairing system key that is *common* to each receiving decoding system in Maillard. In fact, the system of Maillard is not set up to send a common key to multiple receiving units with a decoder and portable security module paired together. This is significant because sending a *different EMM* to each portable security module 3020 requires a large array of EMM's, which in turn requires a large amount of time to send each array of EMM's. Thus, the frequency of validation using the EMM is greatly reduced. In fact, Maillard states that the exploitation key Cex is only changed once a month. (*See* line 65 of column 7 to line 2 of column 8 of Maillard).

The Examiner cites "Maillard, Col. 8 Lines 55 - 63, key pair for decoder and smart card," which discusses a private/public key pairing, as disclosing the pairing system key being common to each receiving decoding system. However, Applicant notes that, although the embodiment shown in Fig. 4 discloses a public key Kpub, Maillard fails to teach the public key Kpub being *common* to multiple receiving decoding systems. (*See* Fig. 4 and line 18 of column 9 to line 17 of column 9 of Millard).

Moreover, Maillard does not validate a combination of the encryption key Kf of the portable security module 3020 and the decryption key Kf of the decoder 2020 by checking for congruence of the combination thereof to a pairing system key. In fact, it appears that Maillard does not send any keys to the portable security module 3020 for the purpose of validating the pairing of the encryption key Kf of the portable security module 3020 and the decryption key Kf of the decoder 2020. Thus, Maillard does not prevent decryption if there is lack of congruence with a pairing system key. Instead, the encryption/decryption process

proceeds as long as the decryption key Kf of the decoder 2020 can decrypt the encryption of the encryption key Kf of the portable security module 3020. Said another way, the claimed invention requires three interconnected keys: a first key unique to a single device, a second key that is determined based on the first key, and a pairing system key to which a combination of the first key and the second key must be congruent in order for the first/second key combination to be validated. In contrast, Maillard has an encryption key Kf and a decryption key Kf, whose pairing is never validated. Instead, upon initialization of the decoder, Maillard simply sends the unique encryption key Kf to the portable security module 3020 based on the decoder identity value N of the decoder 2020, and the validation of the pairing is never verified thereafter. Thus, a hacked encryption/decryption key Kf would be valid indefinitely in Maillard.

Again, the Examiner cites "Maillard, Col. 8 Lines 55 - 63, key pair for decoder and smart card," which discusses a private/public key pairing, as disclosing the combination of the first key and the second key being congruent to a pairing system key. However, Applicant notes that, although the embodiment shown in Fig. 4 discloses a public key Kpub, the system of Maillard does not check for congruence of the public key Kpub with the encryption key Kf and the decryption key Kf. Instead, the public key Kpub is employed to encrypt the pseudo-random number RN generated by the decoder 202, to be decrypted by the private key Kpri stored on the portable security module 3020. In fact, the only connection that the encryption key Kf and the decryption key Kf have with the public key Kpub is that the pseudo-random number RN encrypted by the public key Kpub and decrypted by the private key Kpri is received by the encryption key Kf in the portable security module 3020. Thus, the system of Maillard clearly does not check for congruence of the public key with the encryption key Kf and the decryption key Kf. (*See* Fig. 4 and line 18 of column 9 to line 17 of column 9 of Millard). Accordingly,

Maillard fails to disclose at least the limitations of 1), 2), and (iii), as required by independent claims 1 and 15.

Further, the Examiner admits that Maillard fails to disclose or render obvious a first unique key dedicated to a single device, recited in (ii) above. Applicant agrees that Maillard lacks this particular feature, in addition to the other limitations described above. However, the Examiner relies on Kirkland as teaching a first unique key dedicated to a single device. Applicant respectfully disagrees, and asserts that Kirkland both fails to supply that which Maillard lacks, and also fails to disclose or render obvious that which the Examiner relies on Kirkland as teaching.

Kirkland is directed to a wireless transmission link provided by a wireless bridge device pair, for a secure wireless connection between a data processing system and a network. The Examiner cites paragraph [0005] as disclosing a key unique and dedicated to a single device. However, the cited portion of Kirkland discloses that the two wireless bridge devices *share* a common encryption/decryption key that is unique to the device *pair*. Accordingly, the key mentioned in Kirkland is not unique to a single device, but on the contrary, is unique to a pair of devices. The Examiner's reliance on the cited portion of Kirkland and the logically incorrect equation of the common to a pair of devices key in Kirkland to the unique single device key of the claimed invention requires the Examiner to mischaracterize the teachings of Kirkland or to read out specifically claimed limitations, both of which are improper. Accordingly, Kirkland fails to disclose or render obvious (ii) as required above.

Further, Kirkland also fails to supply that which Maillard lacks. Specifically, Kirkland fails to disclose or render obvious a broadcast system in which a first and second key are each assigned to each of a pair of devices, and that together, form a key congruent to a

pairing system key, as claimed. In fact, Kirkland teaches that a same key is involved in both the transmission side and the receiving side of the wireless communication. This is squarely contradictory to that which is required by the claimed invention, as the claimed invention does not have the same key in the transmitter and the receiver. Thus, Kirkland also fails to disclose or render obvious (iii) as required above.

Accordingly, it is clear that neither Maillard, nor Kirkland discloses the key construction required by (ii) and (iii) above. In fact, Kirkland adds nothing to Maillard, which already describes a pair of unique keys for encrypting the messages. In view of the above, the Examiner's contentions fail to support an obviousness rejection of the independent claims. Pending dependent claims are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 7-10, 17, and 18

Claims 7-10, 17, and 18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Maillard and Kirkland, in further view of U.S. Patent Application Publication. No. 2001/0002486 ("Kocher"). This rejection is respectfully traversed as follows.

As explained above, both Maillard and Kirkland fail to show or suggest all of the limitations of independent claims 1 and 15. Kocher fails to supply that which Maillard and Kirkland lack. Specifically, Kocher discloses an RSA encryption/decryption algorithm. However, Kocher fails to show or suggest a single pairing system key that is *common* to each receiving decoding system, or a first key, a second key determined according to the first key, and a pairing system key to which the combination of the first and second keys must be congruent for decryption to occur.

In view of the above, independent claims 1 and 15 are patentable over Maillard, Kirkland, and Kocher, whether considered alone or in combination, at least for the above reasons. Claims 7-10 and 17-18 are dependent, either directly or indirectly, from claims 1 and 15, and are patentable over Maillard, Kirkland, and Kocher, at least for the same reasons as claims 1 and 15. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 17250/017001).

Dated: September 2, 2011

Respectfully submitted,

By Seema Mehta
for Jonathan P. Osha 56,235
Registration No.: 33,986
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant